Operating Systems
Professor Ward
Spring 2021

Packet Inspection Assignment

Download and install Wireshark. Run it, select an interface with traffic, and start capturing packets. Do a ping, plus a whois or anything else to generate network traffic. Stop the capture.

1. Show a screenshot of Wireshark at the end.

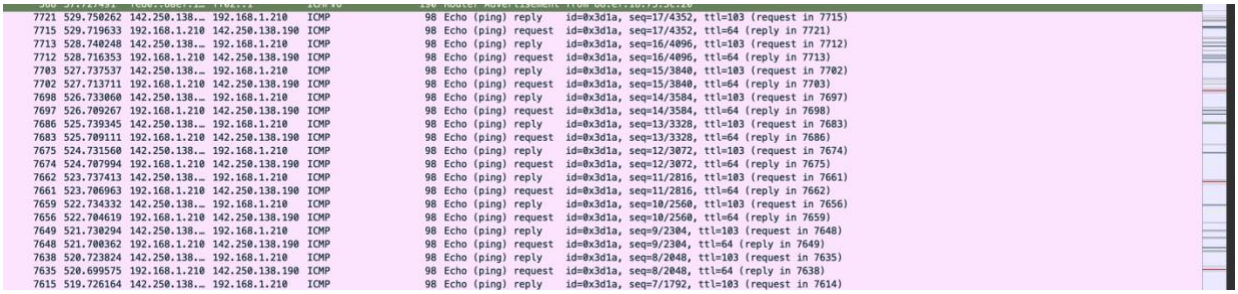
2. How many packets did it capture? What was the packets-per-second rate?

→ 7766 packets

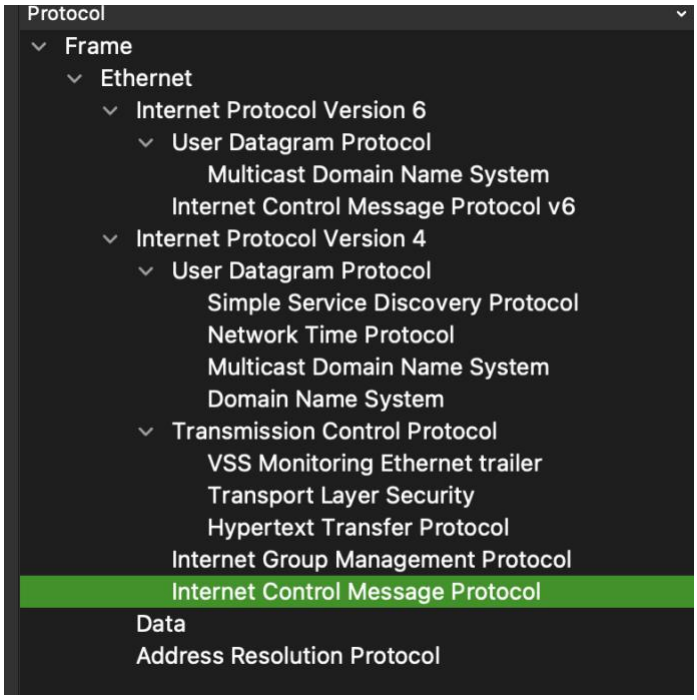
Measurement	Captured	Displayed	Marked
Packets	7766	7766 (100.0%)	—
Time span,s	535.618	535.618	—
Average pps	14.5	14.5	—
Average packet size,B	402	402	—
Bytes	3118522	3118522 (100.0%)	0

3. What protocol is used by ping?

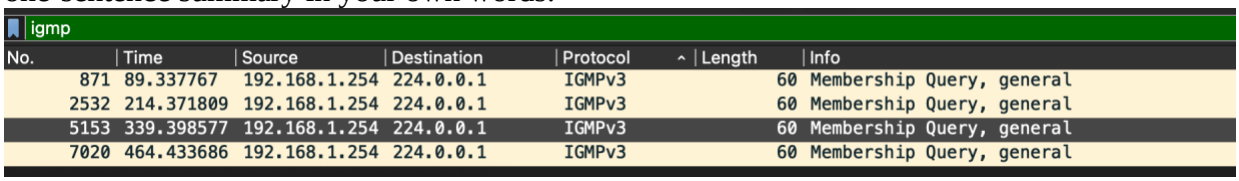
→ uses ICMP protocol



4. List the protocols used by the captured packets.
→ TLS (TLSv1.3, TLSv1.2), TCP, SSDP, NTP, MDNS, IGMP (IGMPv3), ICMP (ICMPv6, ICMP), HTTP, DNS, ARP, 0x7373

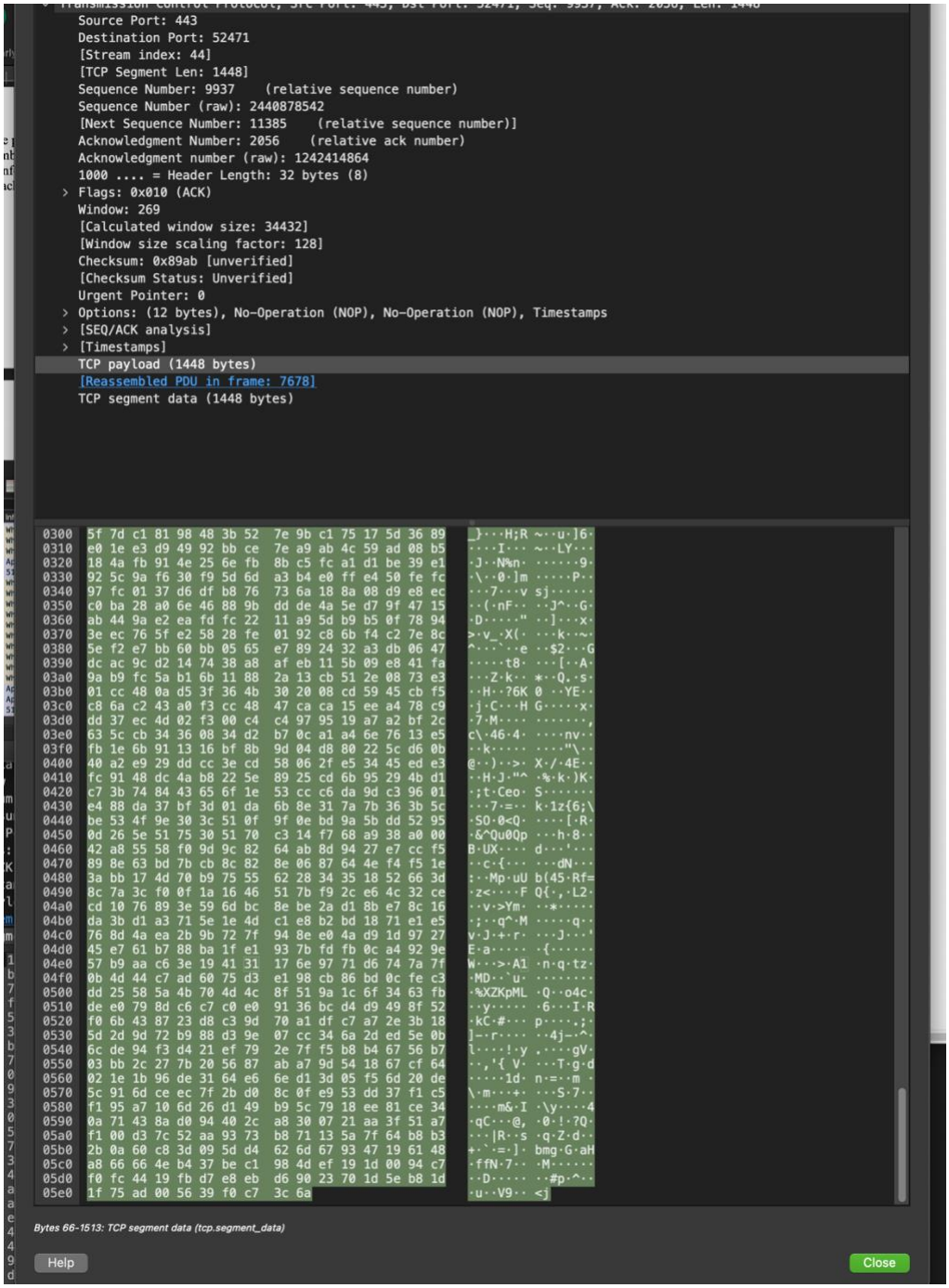


5. Pick one of these protocols which was unfamiliar to you, learn what it does, and give a one-sentence summary in your own words.



→ IGMP: Internet Group Message Protocol --- This protocol is used to allow a host to advertise its multicast group with neighboring switches and routers, which means it lets to communicate from one source to a selected group of destination.

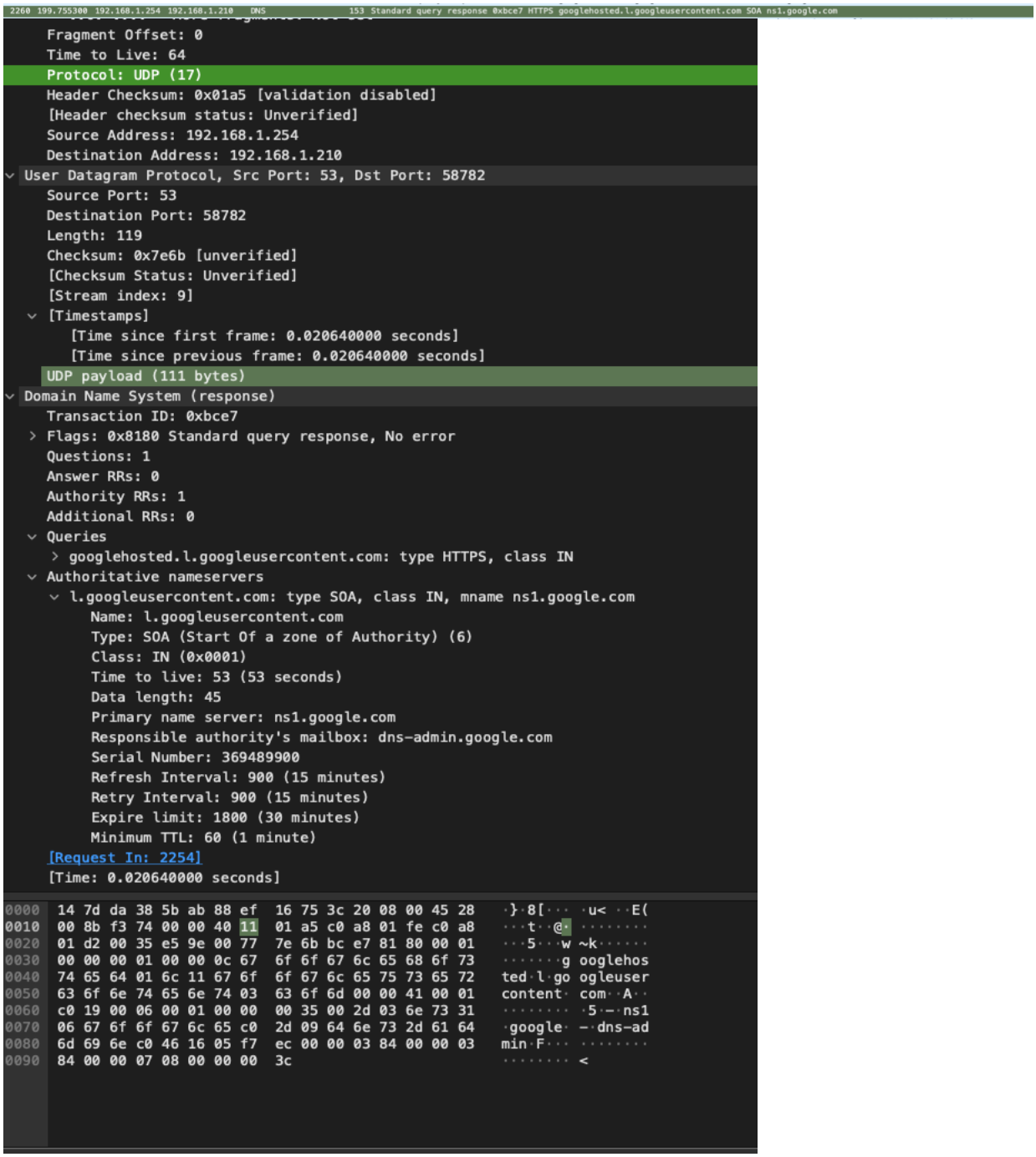
6. Find the longest packet and double click on it. Show a screenshot of the payload, and give your guess as to what this packet is for.
   →



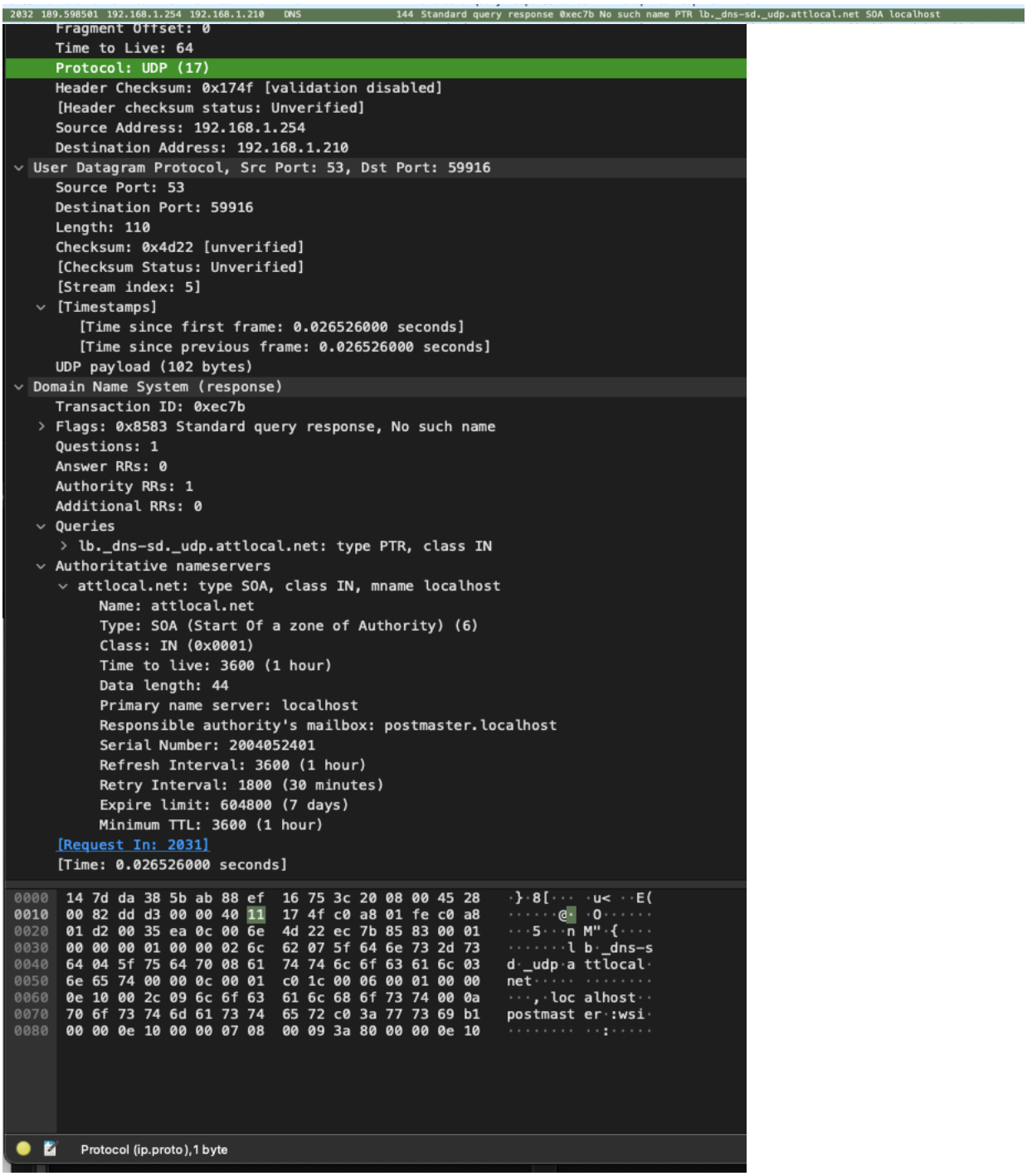
Since the source port is 433, I know that it is an HTTPS (website) packet.

7. Look at any 3 UDP packets. The header should include the protocol number for UDP, namely 17 (11_{16}). Where does this occur (at what byte number)? Is this the same for each UDP packet? Explain why it occurs here, based the information Wireshark displays and your knowledge of the length and layout of packet headers.

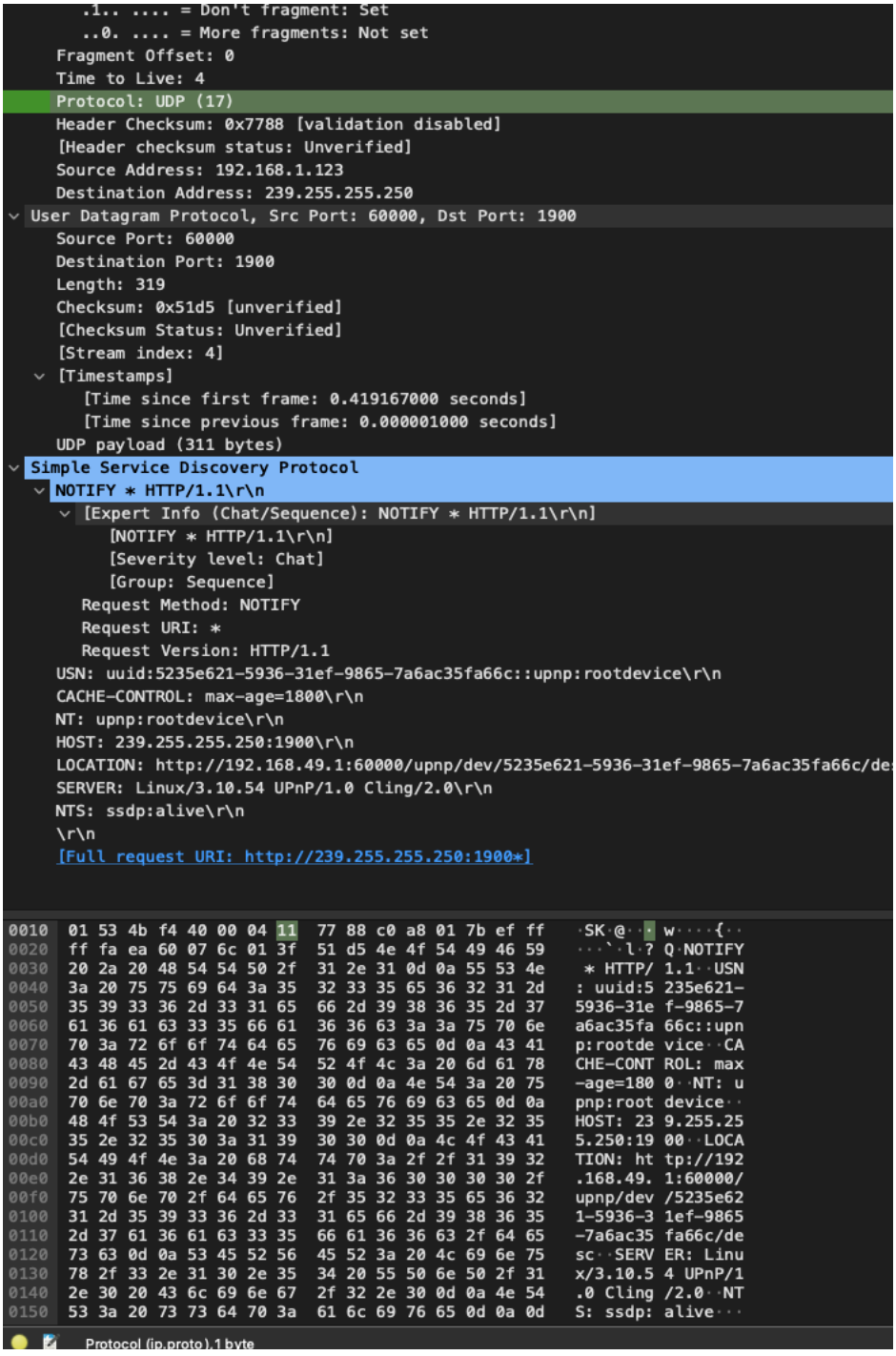
   1.



2.

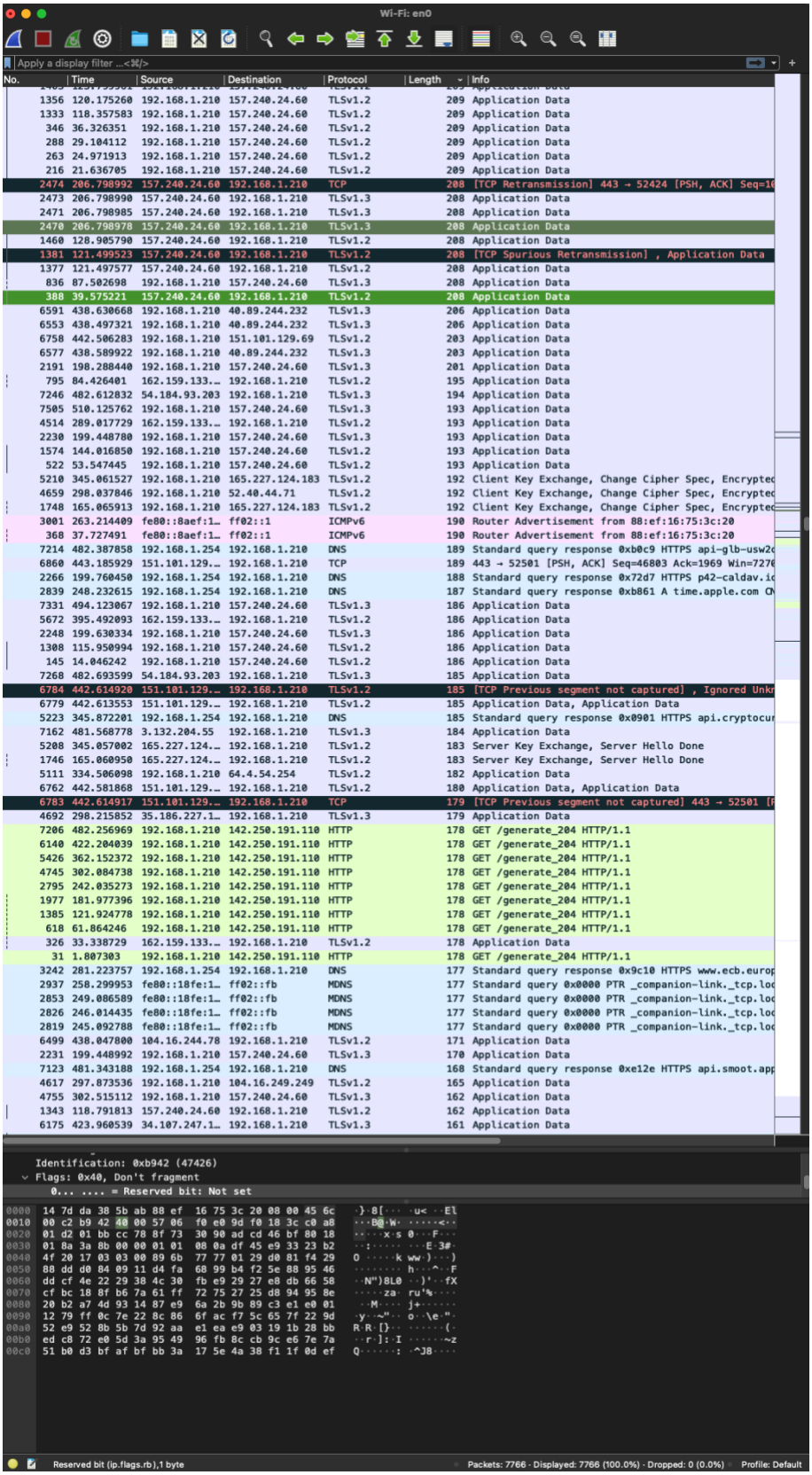

2032 189.598501 192.168.1.254 192.168.1.210 DNS 144 Standard query response 0xec7b No such name PTR lb._dns-sd._udp.attlocal.net SOA localhost
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x174f [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.254
Destination Address: 192.168.1.210
User Datagram Protocol, Src Port: 53, Dst Port: 59916
Source Port: 53
Destination Port: 59916
Length: 110
Checksum: 0x4d22 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[Timestamps]
[Time since first frame: 0.026526000 seconds]
[Time since previous frame: 0.026526000 seconds]
UDP payload (102 bytes)
Domain Name System (response)
Transaction ID: 0xec7b
Flags: 0x8583 Standard query response, No such name
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
lb._dns-sd._udp.attlocal.net: type PTR, class IN
Authoritative nameservers
attlocal.net: type SOA, class IN, mname localhost
Name: attlocal.net
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 44
Primary name server: localhost
Responsible authority's mailbox: postmaster.localhost
Serial Number: 2004052401
Refresh Interval: 3600 (1 hour)
Retry Interval: 1800 (30 minutes)
Expire limit: 604800 (7 days)
Minimum TTL: 3600 (1 hour)
[Request In: 2031]
[Time: 0.026526000 seconds]
0000 14 7d da 38 5b ab 88 ef 16 75 3c 20 08 00 45 28
0010 00 82 dd d3 00 00 40 11 17 4f c0 a8 01 fe c0 a8
0020 01 d2 00 35 ea 0c 00 6e 4d 22 ec 7b 85 83 00 01
0030 00 00 00 01 00 00 02 6c 62 07 5f 64 6e 73 2d 73
0040 64 04 5f 75 64 70 08 61 74 74 6c 6f 63 61 6c 03
0050 6e 65 74 00 00 0c 00 01 c0 1c 00 06 00 01 00 00
0060 0e 10 00 2c 09 6c 6f 63 61 6c 68 6f 73 74 00 0a
0070 70 6f 73 74 6d 61 73 74 65 72 c0 3a 77 73 69 b1
0080 00 00 0e 10 00 00 07 08 00 09 3a 80 00 00 0e 10
Protocol (ip.proto),1 byte

3. 1797 168.397779 192.168.1.123 239.255.255.250 SSDP 353 NOTIFY * HTTP/1.1



→ All of them are 17 indicating that it is an UDP protocol. In addition, all of them occurred on byte 23 and had the number '11'.
Convert 11x to a decimal is: 1*16^1 + 1*16^0 = 16 + 1 = 17 (UDP protcol number).
The position when protocol occurs is at byte 23.

‘Enternet II’ contains 14 bytes which is irrelevant to IPv4 Header, and ‘Internet Protocol Version 4, Src: 192:168:1:254, Dst: 192.168.1.210’ contains 20 bytes which matches with IPv4 header from Version to Destination Address. Within the IPv4 Header, the protocol is located on the 10th. Thus, 14 bytes, “Internet Protocol Version 4’ which comes before IP header information, plus 10 since the order of IPv4 Header format.
10 + 14 = 24. Counting starts from 0, therefore 24 – 1 = 23.
With this information, it make sense why it have 11, 17, and location of 23rd byte.



Picture of a wireshark screen for Question 1.